



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



JUL 14 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense

This memorandum assigns action to implement the recommendations outlined in the final report of the Information Assurance (IA) and Information Technology (IT) Integrated Process Team (IPT) on Training, Certification, and Personnel Management in the Department of Defense (DoD). The IPT, jointly commissioned by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), was tasked to examine issues pertaining to the hiring, retention, training, and certification of IA and IT professionals and was comprised of representatives from 15 DoD Components.

The final report provides 19 recommendations that must be successfully implemented to achieve the desired end-state of sustaining a pool of skilled IA/IT professionals to meet current and future technological needs of the Department. Implementation of some of these recommendations has already begun. The final report dated August 27, 1999, and the report supplement dated February 2, 2000, may be found at <http://www.c3i.osd.mil/org/sio/ia/diap>.

The Commanders-in-Chief (CINCs), Services, and several Agencies have efforts underway to identify, train, and certify their systems administrators. The Services are addressing ways to retain their trained professionals and initial efforts are being taken to work issues regarding Advanced Distributed Learning. IT function codes are being revised and more clearly defined for IT and IA activities. The Joint Staff is developing guidance in the form of Chairman of the Joint Chiefs of Staff Instruction(s) which support these recommendations, and coordination is underway to incorporate IA requirements in DoD Directive 8500.xx, "Information Assurance."

U09310 /00

The attachment lists the recommendations and assigns the lead organization for action, with coordinating organizations identified as appropriate. Lead organizations shall develop an implementation plan for each respective recommendation, taking into account the efforts already underway. Implementation plans are to be finalized and submitted to my office for approval within 90 days.

A consolidated status report on plan execution will be submitted by the ASD(C3I) every 60 days, commencing 60 days after implementation plan approval.

My point of contact (POC) for IT-related recommendations is Ms. Joyce France, telephone 703-604-1491, email: joyce.france@osd.pentagon.mil. For IA-related recommendations, the POC is CAPT J. Katharine Burton, telephone 703-602-9988, email: katharine.burton@osd.pentagon.mil.

A handwritten signature in black ink, appearing to read "Rudy de Leon". The signature is fluid and cursive, with the first name "Rudy" being more prominent than the last name "de Leon".

Rudy de Leon

Attachment

Information Assurance (IA) and Information Technology (IT) Integrated Process Team (IPT) Report Recommendations and Action Assignments

No.	Recommendation	Action	Coordination
1	Establish the requirement that the Commanders in Chief (CINCs), Services, and Agencies (C/S/As) identify manpower and personnel assigned Information Technology(IT)/Information Assurance (IA) functions, enter the required information into the appropriate databases and maintain these databases as changes occur.	OUSD(P&R)	OASD(C3I)
2	Revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities.	OASD(C3I)	OUSD(AT&L) OUSD(P&R)
3	Draft guidance for review by the IGWG to be used by DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability.	OASD(C3I)	
4	Develop and maintain a database that shows contractor staff-years against major functions, especially IT and IA.	OUSD(AT&L)	OASD(C3I)
5	Establish a steering group comprised of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues (i.e., recruiting and retention of IT professionals.	ODASD(MPP)	OASD(C3I)
6	Widely publicize OPM flexibilities (i.e., recruitment bonuses, education benefits, etc.) available to address civilian IT recruiting and retention problems.	ODASD(CPP)	OASD(C3I)
7	Require the staffs of the DoD Chief Information Officers (CIOs) at GS-13 through GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the Information Resource Management College (IRMC).	OASD(C3I)	
8	Issue policy directing the Services/Agencies to implement a mandatory requirement that all DoD CIOs, Deputy CIOs, and Senior Executive Service members/Flag Officers on the CIO staffs, attend DoD-sponsored Information Technology Management (ITM) executive sessions.	OUSD(P&R)	OASD(C3I)
9	Coordinate with responsible offices to provide resources (personnel and funding) to accommodate additional training requirements of the DoD ITM Workforce.	OUSD (Comptroller)	OUSD (P&R) OASD(C3I)
10	Develop an IT contemporary issues training module for the CAPSTONE and APEX training sessions.	OASD(C3I)	The Joint Staff ODASD (CPP)
11	Officially adopt National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security (INFOSEC) Glossary," as the official IA Glossary. The Defense-wide Information Assurance Program (DIAP) will coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department.	OASD(C3I)	

Information Assurance (IA) and Information Technology (IT) Integrated Process Team (IPT) Report Recommendations and Action Assignments

No.	Recommendation	Action	Coordination
12	Review the IA requirements in the context of Joint Vision 2010 (now Joint Vision 2020) and translate these requirements into the Universal Joint Task List (UJTL) and Joint Mission Essential Task List (JMETL).	The Joint Staff	
13	Officially adopt the National Institute of Standards and Technology (NIST) Special Publication 800-16, "Information Technology Security Training Requirements: A Role-and-Performance-Based Model," and the NSTISSI National Training Standards ¹ as the minimum DoD IA training standards.	OASD(C3I)	
14	Establish the requirement that C/S/As establish mandatory training and/or certification programs for the five "critical" IA functions ² using the NSTISSI Training Standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the C/S/As to meet the certification IA training requirement or enhanced by the C/S/A to meet its unique needs.	OUSD(P&R)	OASD(C3I) C/S/As DISA
15	Establish the requirement that no person assigned to a "critical" IA function at the entry level may be granted privileged access until the required IA training is successfully completed.	OASD(C3I)	
16	Establish the requirement that the C/S/As document their certification programs in full and develop the capability to readily produce detailed answers about the status of certifications.	OUSD(P&R)	OASD(C3I)
17	Coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements.	OUSD(P&R)	OASD(C3I) C/S/As
18	Develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at appropriate locations.	OUSD(P&R)	OASD(C3I)
19	Incorporate into the DoD Directive 8500.xx, "Information Assurance," the requirement for contractors assigned "critical" IA functions to meet the same or equivalent certification and training requirements as Department personnel.	OASD(C3I)	

¹NSTISSI(s) No.(s) 4012, "National Training Standard for Designated Approving Authority (DAA)," 4013, "National Training Standard for Systems Administrators in Information Systems Security (INFOSEC)," 4014, "National Training Standard for Information Systems Security Officers (ISSO)," and 4015 (draft), "National Education and Training Standard for System Certifiers."

²IA functions deemed "critical" include System/Network Administration and Operations, Computer/Network Crime, Threat and Vulnerability Assessment, Computer Emergency Response Team (CERT), and Web Security.